

Do not trust me: Using malicious IdPs for analyzing and attacking Single Sign-On

Christian Mainka*, Vladislav Mladenov**, and Jörg Schwenk

Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany
 {christian.mainka,vladislav.mladenov,joerg.schwenk}@hgi.rub.de

Abstract. Single Sign-On (SSO) systems simplify login procedures by using an Identity Provider (IdP) to issue authentication tokens which can be consumed by Service Providers (SPs). Traditionally, IdPs are modeled as trusted third parties. This is reasonable for SSO systems like Kerberos, MS Passport and SAML, where each SP explicitly specifies which IdP he trusts. However, in open systems like OpenID and OpenID Connect, each user may set up his own IdP, and a discovery phase is added to the protocol flow. Thus it is easy for an attacker to set up its own IdP.

In this paper we use a novel approach for analyzing SSO authentication schemes by introducing a *malicious IdP*. With this approach we evaluate one of the most popular and widely deployed SSO protocols – OpenID. We found four novel attack classes on OpenID, which were not covered by previous research, and show their applicability to real-life implementations. As a result, we were able to compromise 11 out of 16 existing OpenID implementations like Sourceforge, Drupal and ownCloud.

We automated discovery of these attacks in a open source tool *OpenID Attacker*, which additionally allows fine-granular testing of all parameters in OpenID implementations.

Our research helps to better understand the message flow in the OpenID protocol, trust assumptions in the different components of the system, and implementation issues in OpenID components. It is applicable to other SSO systems like OpenID Connect and SAML. All OpenID implementations have been informed about their vulnerabilities and we supported them in fixing the issues.

1 Introduction

Single Sign-On. Single Sign-On (SSO) is a technique to enhance and simplify the login process on websites. Instead of managing a plethora of username/password combinations for each website, a user just needs an account at an Identity Provider (IdP) which can then be used to log in on a Service Provider (SP).

* This work has been funded by the European Union within the European Regional Development Fund program.

** The author was supported by the SkIDentity project of the German Federal Ministry of Economics and Technology (BMW, FKZ: 01MD11030).

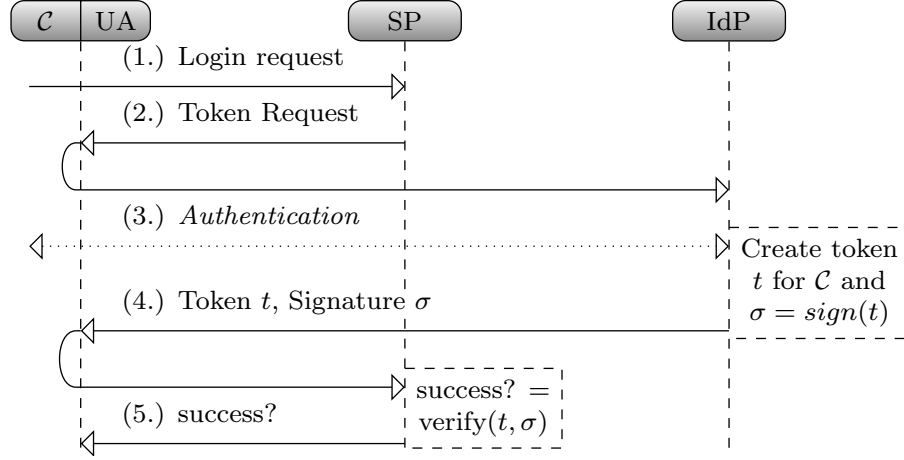


Fig. 1: Single Sign-On (SSO) overview.

Figure 1 gives an overview of a basic SSO scenario. When a client (\mathcal{C}) tries to log in to a service offered by the SP, \mathcal{C} sends a login request (1.) through some user agent (UA) (typically a webbrowser). If \mathcal{C} is not yet authenticated to the SP, a token request is returned (2.). The token request message contains information on the SP, the chosen IdP (e.g. the IdP’s URL) and optionally on \mathcal{C} ’s account name at the IdP. \mathcal{C} ’s user agent is redirected to the IdP and forwards the token request to it. If \mathcal{C} is not yet logged in at this IdP, she/he has to authenticate in Step (3.). The IdP then issues an authentication token t for \mathcal{C} which is commonly protected by a cryptographic signature¹ σ . In Step (4.), t is sent back to the UA, which forwards it to the SP. Finally, the SP verifies t and, in case of successful verification, grants access to its resources in Step (5.).

Motivation. Password based authentication still dominates the Internet, but security problems related to passwords are obvious: Users either use weak passwords or reuse passwords between different sites, password based login is prone to simple attacks like Phishing or dictionary based attacks, and recently two studies on password managers [1,2] showed all of them to be insecure. SSO schemes have been proposed to replace password based authentication, to enhance both usability and security. A recent non-academic overview [3] claims that 87% of U.S. customers are aware of SSO and more than half have tried it. OpenID is one of the most widespread SSO protocols and is currently integrated in 1.2 million websites [4]. Leading companies like Google, Facebook, and PayPal support OpenID based authentication.

The prospect of enhanced security through the introduction of SSO schemes is combined with higher risks because SSO schemes constitute a *single point of attack*: If a weakness in a SSO scheme is detected, a large number of Service

¹ In many specifications, both, Message Authentication Codes (MACs) and Digital Signatures, are summarized under the term *signature*.

Providers on the Internet may be affected simultaneously. Thus from the beginning, SSO schemes have been subject to formal security analysis [5,6]. Wang et al. [7] initiated a new branch of research on SSO protocols by analyzing messages exchanged in (partly undocumented) real-life implementations, which led to the identification of serious logic flaws. They introduced a tool called BRM Analyzer to assist in the analysis of implementations. Their analysis only considered messages that could be seen by the browser, and omitted the information flow between SP and IdP. In their model (and in all other previous work, cf. Section 9), client and SP may be controlled by the attacker, but the IdP is assumed to be trustworthy.

In view of the importance of SSO and OpenID, and of the impact a single vulnerability in a SSO system may have, we re-evaluated existing concepts for analyzing the authentication process. The question we tried to answer was: *Are the methodologies described in the literature complete in the sense that there are not other options to attack OpenID?*

New SSO Attacker Paradigm. Since in OpenID it is very easy for anyone to run an IdP, we extended the attack methodology and considered malicious IdPs as well. By running a malicious IdP, we enhance the attacker’s capabilities: he is able to read and manipulate all messages exchanged between a honest SP and the malicious IdP, even for messages that do not pass through the browser (cf. Figure 2). Thus, the attacker has better control over the SSO message flow, which results in a more thorough security analysis of SSO.

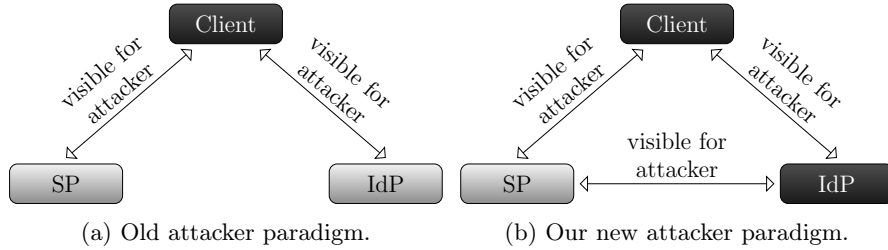


Fig. 2: Our new attacker paradigm uses a *malicious IdP* and can thus see all relevant messages.

This novel approach for attacking an SP revealed four new attack classes: Token Recipient Confusion, ID Spoofing, Key Confusion and Discovery Spoofing. All attacks work in the web attacker model or in even weaker variants. Thus the practical impact of these attacks is very high: For Token Recipient Confusion, the OpenID accounts of any user who visits the attackers web page can be compromised. For ID Spoofing, Key Confusion and Discovery Spoofing, the effect is even more devastating: We can fully compromise *all* accounts on an OpenID SP, *without any user interaction*.

Methodology. After an initial white-box analysis of the different OpenID implementations, we used our own IdP to perform realistic black-box tests against running target SP implementations. For that purpose we used our automatic security testing tool **OpenID Attacker** (Section 8), allowing us to apply all presented attack classes on arbitrary SPs. The results of both analysis phases were then verified as follows: We set up a victim account on each SP implementation, and verified in each case that we could access this account through a second (attacker-controlled) browser, running on a different PC without the victim’s credentials.

The validity of all attacks found has strictly been verified in the *Web attacker model* [8]: The attacker only controls the incoming and outgoing messages to and from web applications which he controls (e.g. malicious clients, SPs and IdPs); all other network traffic is unknown to him. He can also freely access victim web applications through their interface exposed in the WWW, through a web browser or a modified HTTP client. An attack is considered successful if the attacker gets illegitimate access to protected resource at the legitimate SP.

We do *not* assume full control over the network, for instance, we do not use the (stronger) standard cryptographic attacker model, which yields weaker results. Additionally, we do not consider phishing attacks – the attacker does not imitate a legitimate SP and we do not trick out a victim to use the attacker controlled IdP.

Results. We were able to find four novel attacks on OpenID:

- *Token Recipient Confusion* introduces an attacker acting as a malicious SP. The attacker then forwards the received tokens to other SPs.
- *Key Confusion* exploits a vulnerability in the key management implementation of the SP, resulting in the use of an untrusted key. The attacker acts as a malicious IdP.
- *ID Spoofing* introduces an attacker in the role of a malicious IdP, generating tokens in the name of other (trusted) IdPs.
- *Discovery Spoofing* exploits the usage of untrusted identities transmitted during the discovery phase by using a malicious IdP.

We evaluated these attacks against 16 implementations mainly taken from the official OpenID Wiki [9]. Table 1 summarizes the results: were able to compromise 11 of them. Our results show that the verification of a security token is a nontrivial task in OpenID: Dependencies between different data structures must be taken into account (e.g. association name and association key) and REST parameters must be checked with great care (Section 10).

Responsible Disclosure. All vulnerable projects have been informed and most acknowledged our findings. In case we did not receive any reaction, we filed a CVE. We cooperated by proposing and providing bug fixes, which were applied in some cases [10,11,12,13,14,15,16,17,18,19,20,21].

Contribution. The contribution of this paper can be summarized as follows:

- ▶ We propose a novel attacker paradigm for the analysis of SSO protocols – the use of a malicious IdP. As a result, the security evaluation is more comprehensive.
- ▶ We describe four novel attack classes on OpenID by using a malicious IdP, all strictly in the Web attacker model. These attacks provide novel insights into the problems of token verification for SPs, and of enforcing the message flow intended by the OpenID specification.
- ▶ We give a systematic overview on OpenID security and show that roughly 68% of the analyzed implementations are vulnerable, including Sourceforge, Drupal and ownCloud.
- ▶ We contribute to a better understanding of SSO, especially the trust establishment between IdP and SP during the discovery and association phases in OpenID.
- ▶ We develop OpenID Attacker, a free and open source malicious OpenID IdP capable of executing our novel and previous discovered attacks [22].

Outline. In the following section, we present the computational and security model and describe our new SSO attacker paradigm. Section 3 introduces OpenID and the protocol flow. In Section 4, we elucidate the verification processes of authentication tokens and provide a general analysis for SSO. In Section 5, we present novel attacks regarding SSO. The methodology of analyzing SSO systems will be expounded in Section 6. The results of the provided evaluation are supplied in Section 7. Section 8 delineates the implementation of our tool, OpenID Attacker. Related work is discussed in Section 9. In Section 10 we sum up the lessons that we can learn from the paper. Finally, we conclude in Section 11.

2 Computational and Security Model

Computational Model. Figure 1 shows a basic SSO login procedure. However, the real world is more complex and includes multiple clients, SPs, and IdPs. Figure 3 illustrates this scenario. Please note that while each SP may trust several IdPs, and each IdP may serve many SPs, each client’s ID belongs to exactly one IdP.

In OpenID, there is (in contrast to other SSO systems) an “open” trust relationship between SP and IdP: The SP trusts tokens created by any \mathcal{IdP} , as long as $\text{URL}.\mathcal{IdP}$ is contained in the document retrieved from $\text{URL}.\text{ID}_C$. Thus it is easy to inject a malicious IdP \mathcal{IdP}_A into this ecosystem by simply creating a new (malicious) client ID where the discovery document points to $\text{URL}.\mathcal{IdP}_A$. Additionally, we can also run a malicious SP \mathcal{SP}_A . Since we now control each

type of communicating entities in an OpenID system, we also control (and are thus able to modify) all types of messages. This is especially important in the *Analyzing Mode* (cf. Section 8), where we modify certain parameters in each message type and test it against a honest instance of an SP.

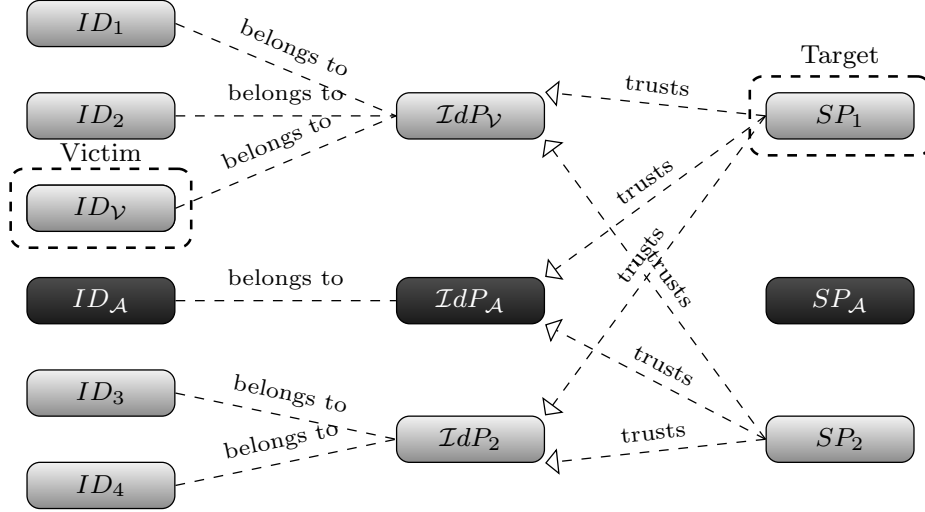


Fig. 3: SSO in the real world involves multiple clients, multiple IdPs and multiple SPs. SP_1 can even *trust* tokens of IdP_A , but only for its corresponding clients, i.e. ID_A .

Please note that control over *all types of messages* should not be confused with control over *all messages*: As Figure 3 shows, we cannot access messages exchanged between honest parties (e.g. IdP_2 and SP_2).

SSO Attacker Paradigm. The goal of the attacker is to access a protected resource to which he has no entitlement. To achieve this goal, he may use the resources of a web attacker only: he can set up his own web applications and he can lure victims to them. Furthermore, in three of four attacks described in this paper (IDS, KC and DS) the attacker is even more powerful: by using the malicious IdP only, the attacker can break into every OpenID account on the target SP without any victim’s interaction. Thus, there is no possibility for the victim to detect or mitigate the attacks.

In an SSO environment, the web attacker can play different roles (Figure 3): (1.) **Malicious client.** He can start an SSO session like any other client. Note that the attacker’s identity ID_A belongs to IdP_A , but the victim’s identity ID_v belongs to IdP_v . (2.) **Malicious IdP.** The malicious IdP (IdP_A) in our model is able to generate valid as well as malformed authentication tokens (attack tokens). (3.) **Malicious SP.** In our experiments, we never used any spe-

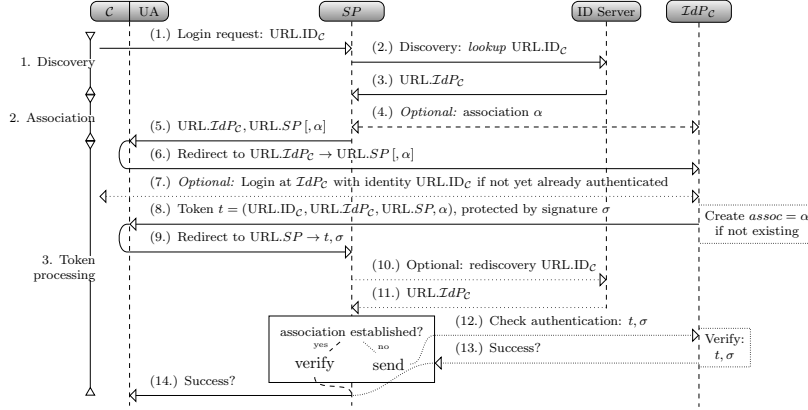


Fig. 4: The OpenID protocol flow.

cial properties of SP_A : it is sufficient that the attacker just controls a domain ($URL.A$).

3 OpenID: Technical Background

OpenID [23] is one of the main SSO standards. In contrast to OAuth and SAML, where a trust relationship between an SP and an IdP needs to be established beforehand, OpenID does not require any registration or configuration at the SPs. OpenID is available as a module for content-management systems (CMSs) like WordPress and Joomla, or it is even directly shipped with the application, for example, with Drupal and ownCloud. Libraries for all commonly used Web programming languages are available [9]. Millions of users already own an OpenID as, for instance, Google, Yahoo, and AOL automatically assign one to each user.

Notation. In OpenID, an identity of a client C is represented by a URL. Therefore, we define it as $URL.ID_C$. Correspondingly, we define the URL of a client's IdP by $URL.IdP_C$ and for an SP, we use $URL.SP$.²

Protocol. OpenID consists of three phases as shown in Figure 4. In the **discovery** phase, the SP collects information about C 's requested identity ($URL.ID_C$) and determines $URL.IdP_C$. In the **association** phase, the SP and the IdP establish a shared secret α intended to be used for signing and verifying the token. The **token processing** phase then includes the creation of the token by the IdP, its transport to the SP via C 's UA, and its verification by SP. Figure 4 describes the OpenID login process more precisely:

- (1.) C wishes to access a resource at the SP and enters his identity $URL.ID_C$.
- (2.) The SP then starts the discovery by requesting the document at $URL.ID_C$.

² $URL.ID_C$ and $URL.IdP_C$ need not necessarily belong to the same domain.

- (3.) A document containing $\text{URL.IdP}_{\mathcal{C}}$ is returned.
- (4.) Using $\text{URL.IdP}_{\mathcal{C}}$, the SP can establish an association with the IdP. This is basically a Diffie-Hellman key exchange to establish a *shared secret* s . Additionally, the IdP freely chooses a string α that is used as a name for the association. It is used to reference the key material k derived from s on both sides, and has an expiration time. Note that in this phase, the SP and the IdP are directly communicating with each other, which means that a web attacker cannot interfere with this communication.
- (5.) Afterwards, the SP has all necessary information to validate an OpenID token created by $\text{IdP}_{\mathcal{C}}$. It responds to \mathcal{C} 's initial login request of Step (1.) and sends an *authentication request* containing $\text{URL.IdP}_{\mathcal{C}}$, URL.SP and optionally α .
- (6.) \mathcal{C} is redirected to $\text{URL.IdP}_{\mathcal{C}}$.
- (7.) If \mathcal{C} is not yet logged in, he must authenticate to $\text{IdP}_{\mathcal{C}}$.
- (8.) $\text{IdP}_{\mathcal{C}}$ creates a token t for \mathcal{C} containing \mathcal{C} 's identity $\text{URL.ID}_{\mathcal{C}}$, its own URL address $\text{URL.IdP}_{\mathcal{C}}$ and URL.SP . $\text{IdP}_{\mathcal{C}}$ then generates a signature σ for t using the key referenced by α . Message (8) is called the *authentication response* and is sent as an HTTP redirect to URL.SP .
- (9.) The authentication response is forwarded to the SP.
- (10.)-(11.) The SP can optionally start a rediscovery, for example, if it has not cached the previous discovery, cf. Step (2.)-(3.).
- (14.) If the signature is valid, the SP will map $\text{URL.ID}_{\mathcal{C}}$ to a local identity and respond accordingly to \mathcal{C} .

Direct Verification. Establishing an association is optional according to the OpenID standard. If the communication (4.) is missing, the authentication request does not contain α , and no *shared secret* was established with $\text{IdP}_{\mathcal{C}}$. In this case, the IdP generates a fresh key and signs the token with it. In this case, the SP will not be able to verify the authenticity of the token by itself. Instead, it must send the token directly to the IdP in Step (12.), and accepts the result of the verification from Step (13.).

Discovery in Detail. To receive $\text{URL.IdP}_{\mathcal{C}}$ in Step (2.), the SP fetches the document at $\text{URL.ID}_{\mathcal{C}}$ (e.g. <http://myserver.org>). This can be either an HTML or an XRDS document. Listing 1.1 shows a minimal HTML document.

```
<html><head><title />
<link rel="openid2.provider"
      href="https://myidp.com/" />
</head><body/></html>
```

Listing 1.1: Minimal HTML discovery document.

The element `<link/>` contains `URL.IdPC` within the `href` attribute. XRDS documents contain the same information, but stored in XML data format.

Note that Step (5.) of the protocol does not contain `URL.IDC`. This is not necessary, since \mathcal{C} must authenticate to \mathcal{IdP}_C . Consequently, \mathcal{IdP}_C knows the value of `URL.IDC`. However, the discovered document in Step (3.) allows optionally to include a second “local” identity `URL.IDC*` (the value of the `href` attribute in Listing 1.2):

```
<link rel="openid2.local_id"
      href="https://myidp.com/bob" />
```

Listing 1.2: \mathcal{C} ’s identity stored in an HTML document.

If this is the case, steps (5.) and (6.) will include this value as well and \mathcal{IdP}_C is asked to use `URL.IDC*`. This is, for example, useful if \mathcal{C} owns multiple IDs at \mathcal{IdP}_C .

4 SSO Token verification

Token verification at the SP is the most critical part within the SSO process. It consists of many steps in order to guarantee the validity of the authentication. This observation holds for SSO in general (SAML, OAuth and OpenID). In the following, these verification steps are discussed.

Message Parsing. Each token has a specific structure. For instance, each OpenID parameter starts with `openid.*`, and the required set of parameters must be checked by each application. At the beginning, whenever an SP receives a message, it has to be parsed into a data object so that it can be processed further. Any error during this parsing directly affects SSO security: for instance, if some data element is present twice with different content, the second content may overwrite the first during the parsing, or vice versa. Additionally, all required parameters must be present.

Freshness. Freshness of authentication tokens is important for preventing replay attacks. It can be realized with two parameters: (1.) a nonce, which is a random value selected by the SP and/or (2.) a timestamp which defines the token’s creation time or period of validity, and which is usually selected by the IdP. OpenID uses the parameter `openid.response_nonce`. It contains the creation time of the token concatenated with a random string.

Token Recipient Verification. A token t is intended for a single SP. Thus, it should be guaranteed that (1.) t can be successfully verified by a single SP only, and (2.) that t is delivered to the correct SP. OpenID uses the `URL.SP` parameter for purpose (1.). This parameter should be checked by the SP. For (2.), the HTTP-Receiver of the redirect message sent by the IdP is given in the OpenID parameter `URL.SP`. Here the IdP must check that this parameter is valid.

IdP Verification. The SP receiving a token should verify: (1.) the origin of the received token and (2.) the validity of the statements contained. (1.) is verified

in three steps: (1.1) The SP must determine the unique identity of the IdP (e.g. an URL) which issued the authentication token. (1.2) The SP must fetch the corresponding key material associated to that identity. (1.3) Using this key material, the signature of the token is verified. In (2.) the SP should verify whether the IdP is allowed to make the statements in the token, for example, $\mathcal{IdP}_{\mathcal{A}}$ must not issue tokens in the context of $\mathcal{IdP}_{\mathcal{V}}$.

Cryptographic Token Verification. For step (1.3) above, the signed parts must be determined. The SP must be able to distinguish signed from unsigned parts within the token. For instance, in OpenID, it should be able to distinguish signed HTTP header fields from unsigned ones. Additionally, it should check if all parameters that are required to be signed are indeed signed.³

For step (1.2) above, the right keys must be chosen. The SP uses the key material associated with the selected IdP. If this association between key material and identity can be overwritten (cf. Section 5.2), novel attacks are feasible.

5 Novel Attacks

In this section, we give generic descriptions of four novel attacks on OpenID, which are effective against different implementations of OpenID (cf. Table 1). The first two attacks, Token Recipient Confusion and Key Confusion, are protocol independent and can be applied to other SSO protocols. ID Spoofing and Discovery Spoofing exploit characteristic of OpenID.

5.1 Token Recipient Confusion

Token Recipient Confusion (TRC) attacks as shown in Figure 5 target a missing URL.SP parameter verification. This violates condition (2.) of the *token recipient verification* step (cf. Section 4).

Detection phase. The attacker uses $\mathcal{IdP}_{\mathcal{A}}$ and generates tokens containing identity $\mathcal{ID}_{\mathcal{A}}$. Additionally he sets the value of URL.SP to an arbitrary URL (different from the URL of the target SP) and sends the token to the target SP. Finally, he observes the behavior of the target SP: If the SP accepts the token, then the value of URL.SP is *not* validated, and TRC is applicable.

Exploit phase. In order to exploit the vulnerability, the attacker \mathcal{A} sets up a web application running on URL.A (e.g. a weather forecast service), to initiate an OpenID authentication and to collect authentication tokens. The exact protocol flow is shown in Figure 5.

- (1.) The victim client ($\mathcal{C}_{\mathcal{V}}$) accesses the web application deployed on URL.A .
- (2.) The attacker creates a *Token Request* containing $\text{URL.SP} = \text{URL.A}$.
- (3.) $\mathcal{C}_{\mathcal{V}}$ authenticates to $\mathcal{IdP}_{\mathcal{V}}$. If he is already authenticated, this step is skipped.

³ In the context of SAML, this has been shown to be quite challenging [24].

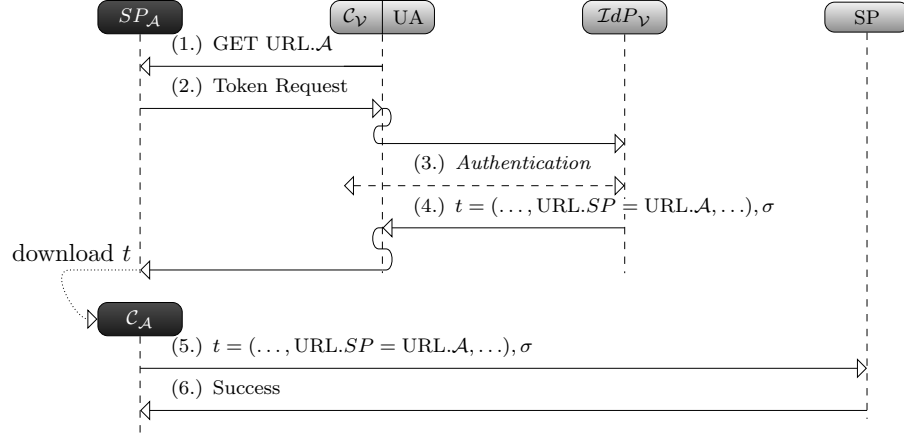


Fig. 5: Token Recipient Confusion Attack.

(4.) IdP_V generates the token t and sends it back to C_V , with a redirect to $URL.SP = URL.A$. The client's UA executes this redirect, and thus sends the token to A .

(5.) Finally, C_A downloads the collected token t, σ from SP_A and uses it to log in on the target SP.

Note that in case that C_V is already authenticated to IdP_V , Steps 2,3,4 and 5 will be executed without any user interaction.

TRC is a generic attack and can be adapted to other SSO protocols like SAML and OAuth, since these include parameters similar to $URL.SP$. For SAML, this is the *AssertionConsumerServiceURL* parameter [25, Section 3.4.1] which is already evaluated in [26]. In OAuth, the parameter is called *redirect_uri* [27, Section 4.2.1].

To mitigate the TRC attack, the SP should verify whether the $URL.SP$ parameter contained in t matches its own URL.

5.2 Key Confusion

Key Confusion (KC) is a generic and very complex attack on SSO. A detailed example is shown in Figure 7. The goal of the attacker is to force the target SP to use a key of the attacker's choice to verify a (forged) token t^* . To achieve this goal, he must agree a common secret key (or a public key) with the target SP, and thus play the role of a (malicious) IdP. Then he may follow one of two strategies to succeed. KC attacks address the second part of the *cryptographic token verification* step (cf. Section 4).

Strategy 1. *Overwriting the secret key handle of a trusted IdP.* In the case of OpenID, the key material is referenced by the association handle parameter α . Since the value of α is chosen by the IdP (and not by the SP), the attacker

(acting as a malicious IdP) is able to set α to the same value as defined by the valid IdP in order to overwrite it with its own key values. The attacker may get to know the original α by starting an attempt to log in as the victim on the target SP. He will then receive α in message (5.) of Figure 4.

Strategy 2. *Submit attacker's own key handle for signature verification.* The association α is also part of the signed token t^* . Thus, some SP implementations are tempted to use this value to verify the signature. The fact that the token may be issued by a malicious IdP clearly shows that this leads to a critical vulnerability: If a malicious $\mathcal{IdP}_{\mathcal{A}}$ issues the token $t^* = (\text{URL.ID}_{\mathcal{V}}, \text{URL.IdP}_{\mathcal{V}}, \text{URL.SP}, \beta)$ and protects it with a signature key related to β , the target SP may accept this token. Although $\mathcal{IdP}_{\mathcal{A}}$ is not entitled to issue such tokens. This behavior is not clearly prohibited: According to the OpenID specification [23, Section 11.2], an SP should verify that the discovered information (user's identity and IdP's URL) maps the presented content in the received token. Unfortunately, this check does not verify that the key used for signing the token belongs to the discovered IdP.

The idea of KC can be adapted to other SSO protocols using digital signatures for integrity protection, for example, SAML [28, Section 4.4.2].

5.3 ID Spoofing

ID Spoofing (IDS) is an OpenID specific attack. Its goal is to create a token t^* containing the victim's identity ($\text{URL.ID}_{\mathcal{V}}$) by using the attacker's IdP. It is successful if the target SP accepts t^* . Given the simplicity of this attack it is surprising that it has not been described before. IDS attacks target condition (2.) of the *IdP verification* step (cf. Section 4).

In OpenID, a user's identity is represented by $\text{URL.ID}_{\mathcal{V}}$, which is controlled by exactly one IdP ($\mathcal{IdP}_{\mathcal{V}}$ with $\text{URL.IdP}_{\mathcal{V}}$). Consequently, an IdP can make statements only for user identities bound to its domain. Thus, $\mathcal{IdP}_{\mathcal{A}}$ should in theory not be able to create a valid token t^* containing $\text{URL.ID}_{\mathcal{V}}$. For OpenID, the corresponding check should work as follows: According to the specification [23, Section 11.2], an SP should start a (second) discovery on the identity $\text{URL.ID}_{\mathcal{V}}$ contained in t^* . In this manner, SP can discover whether $\text{URL.ID}_{\mathcal{V}}$ belongs to the IdP contained in t^* , i.e. $\mathcal{IdP}_{\mathcal{A}}$ in this case. If this step is not implemented properly, an attacker is able to inject identities, which are not controlled by his malicious IdP. In this manner, the attacker can impersonate users with different, trustworthy IdPs, for example, Google or Yahoo, by using only his own $\mathcal{IdP}_{\mathcal{A}}$.

5.4 Discovery Spoofing

Discovery Spoofing (DS) is an attack which is only possible if the SP uses the second "local" $ID_{\mathcal{C}}^2 = \text{URL.ID}_{\mathcal{C}}^*$ for identifying the client. The OpenID specification allows this usage of identity $ID_{\mathcal{C}}^2$ returned by the ID server [23, Section

10.1]. The attack exploits the fact that this second ID_C^2 cannot be used for discovery: Only the first ID_C^1 uniquely determines the trusted IdP. The attack can be outlined as follows (a detailed description is given in Section 7.4):

- (1.) The attacker stores a (malformed) XRDS/HTML document on his ID Server containing the victim's second identity $ID_V^2 = \text{URL.ID}_V$ (see Listing 1.2). This document can be retrieved through $ID_A^1 = \text{URL.ID}_A$.
- (2.) The XRDS/HTML document thus retrieved points to an Identity Provider $\text{IdP}_A = \text{URL.IdP}_A$ under the control of the attacker.
- (3.) IdP_A issues a valid token t for ID_A^1 , and the target SP successfully verifies t . To match this verification to a local identity, the attacker must either perform another (second, optional) discovery using ID_A^1 , or retrieve the result of the first discovery. In both cases, he will get the local ID ID_V^2 , and consequently grant access to A .

6 Methodology

Target SPs. We selected 15 open source implementations including libraries and frameworks that support OpenID, mainly taken from the official OpenID website [9]⁴. We tried to cover every available language: Our list contains implementations in .NET, C++, ColdFusion, Java, JavaScript, Perl, PHP, Python, and Ruby. We added Drupal to the target list, since it is a widely used CMS and has a custom implementation of OpenID. The only implementation that did not permit a white-box analysis is Sourceforge [29]. We included it because it is a very prominent site supporting OpenID (Alexa [30] rank 160) and because it does not use one of the inspected implementations listed on [9].

White-Box Tests. We used white-box tests to analyze the source code and the protocol flow of each target. Based on the white-box tests, we developed the concepts for the attack classes described in Section 5 and implemented them in OpenID Attacker.

Setup. For each implementation, we created a working virtual web server/virtual CMS server, and deployed the framework in it. For Sourceforge, we used the live website.

We registered two accounts on each target as shown in Figure 6: As victim V , we used an account at a trusted IdP to register a local account on the target SP. Using a second browser on a different PC we registered a second account for A at the target SP, associated with an account on our custom malicious IdP – the OpenID Attacker account.

⁴ Note that some of the libraries are listed multiple times, for example, libopkele is the module used in Apache mod_auth_openid, the listed Python Django OpenID framework uses janrain etc.

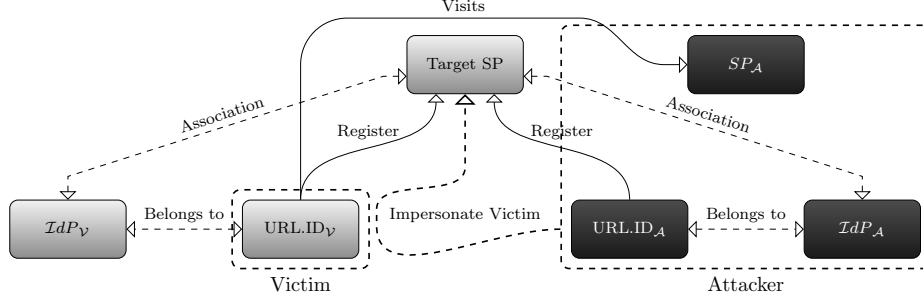


Fig. 6: Evaluation setup and goal.

In this step, the second account was mainly used to verify that the OpenID Attacker IdP is working flawlessly and that the target is able to verify valid tokens created by our tool.

Black-Box Test using OpenID Attacker. Offering the ability to manipulate each parameter in every phase of the OpenID protocol, OpenID Attacker (cf. Section 8) allows to evaluate the token verification of an SP in a very flexible way. The tokens to attack the target SP are created automatically. We varied several parameters selected according to our white-box analysis, until the attack was working.

Exploit. Finally, we performed the attacks in the web attacker model: For only one attack (TRC) it is necessary that victim \mathcal{V} visits a web page SP_A under control of the attacker \mathcal{A} . In our setting, \mathcal{V} is already authenticated to the trusted IdP (stored in a session cookie), so that no explicit authentication of \mathcal{V} is necessary. We verify that the token t is indeed transferred to SP_A , and that we could use this token from our second browser to gain access to the target SP.

To verify KC attacks, we have sketched two strategies in Section 5. For following the first strategy, the precondition that an association α exists between the target SP and the trusted IdP must be fulfilled. We can get the value of α in message (5.) of Figure 4 when we try to log in with the victim's identity. This attempt will not succeed, but we can see message (5.) nonetheless. We then established a new association between the target SP and OpenID Attacker using the same α and analyzed whether the target SP afterwards accepted our malicious tokens as valid for \mathcal{V} . For the second strategy, only an association β between the target SP and the malicious IdP is necessary. We verified that the SP accepted tokens containing $(URL.ID_V, URL.IdP_V)$ that were signed with the malicious association β .

For the two remaining attacks (IDS, DS), we only needed to know the first and second identity of \mathcal{V} . We verified that the target SP accepted our malicious tokens for these two identities.

7 Practical Evaluation

We reported all vulnerabilities to the liable security teams and to the Computer Emergency Response Team (CERT). In case we got a response from the developers, the time to fix the reported issues ranged between a few days and several months. Furthermore, we supported the developer teams during fixing the reported issues.

Our results are summarized in Table 1: for 11 out of 16 targets, we were able to access a protected resource. On eight of the eleven targets an attacker can compromise *all* of the accounts, without any user interaction. On the other three targets the account of any victim can be compromised, if he visits a malicious website.

7.1 Token Recipient Confusion

We analyzed the processing of the $URL.SP$ -parameter. To verify this vulnerability, we configured our custom IdP to create a token containing $URL.SP_A$ instead of the correct $URL.SP$. If the token was accepted, we categorized the TRC attack scenario as applicable: 6 out of 16 OpenID targets were susceptible to the described TRC attack.

JOID. JOID [31,12] is a free open source library supporting OpenID authentication. At first, we evaluated whether the library verifies the $URL.SP$. For that purpose, we used the OpenID Attacker and configured it to create a token containing $URL.A$ instead of the original $URL.SP_{JOID}$. Since the JOID SP running on $URL.SP_{JOID}$ accepted the token, we started the second step of the analysis – the exploit:

- (1.) In the role of the attacker, we upload a website containing a PHP script, which is available from the Internet by visiting $URL.A$, see Figure 5.
- (2.) We then simulate the victim who visits $URL.A$ from a different PC. For testing, we used a Yahoo account. The attacker’s PHP script generates a *Token Request* for the victim containing $URL.SP = URL.A$ and then redirects him to $URL.IdP_{Yahoo}$.
- (3.) Still in the role of the victim, we do not need to authenticate to the IdP according to the methodology, see Section 6. Afterwards, the IdP generates the OpenID token $t = (URL.ID_V, URL.A, \dots)$. Then, the IdP redirects the victim together with t to the SP, using $URL.A$ from the *Token Request* – the victim sends t to the attacker’s script.
- (4.) Once the script receives t , the attacker sends t to the inspected JOID SP. Although $URL.A \neq URL.SP_{JOID}$, JOID accepts t and the attacker is logged in with victim’s account.

7.2 Key Confusion

Three targets were vulnerable to Key Confusion (KC): Drupal, Zend Framework and Sourceforge. These implementations used a key belonging to OpenID Attacker for verifying the signature instead of using the key belonging to the victim's IdP. The attack on Drupal worked as follows:

Drupal. Drupal [32] is a free open source CMS. It is based on PHP and according to [33], it is the third most frequently used CMS. Famous sites using Drupal are Twitter (Alexa rank 11) or Typepad (Alexa rank 498). Its OpenID support is shipped with every Drupal distribution and just needs to be activated within the settings menu.

We started to analyze the implementation by carrying out the TRC, but it failed. Then, we tried to apply the IDS attack: We submitted $URL.ID_A$ on the Drupal login form. The SP starts the discovery on it and receives $URL.IdP_A$ belonging to our OpenID Attacker IdP. Drupal redirects us to it, but instead of creating a token for $URL.ID_A$, it creates a token $t^* = (URL.ID_V, \dots)$ containing the victim's Google identity. Sending t^* to Drupal did not succeed. Drupal noticed that the originally submitted identity $URL.ID_A$ differs from the value $URL.ID_V$ contained in t^* . As a result, Drupal starts a second discovery on $URL.ID_V$, which returns $URL.IdP_V$. Drupal compares this value to $URL.IdP_A$ returned by the first discovery. Since the values are not equal, we are not logged in. Interestingly, Drupal does *not* compare the discovered value with the value $URL.IdP$ contained in t^* , thus sending a token $t^* = (URL.ID_V, URL.IdP_V, \dots)$ also fails.

In order to prevent the second discovery process, which mitigates the attack, we did a white-box analysis of the source code. We found out that Drupal uses the PHP `$_SESSION` variable to store and load $URL.ID$ and $URL.IdP$. In this manner, Drupal links both messages: the login request and the received token.

The `$_SESSION` variable is a globally available PHP array which holds arbitrary session data on a per-user basis. Whenever Drupal receives an OpenID token t^* , it first verifies if the $URL.ID$ parameter, contained in t^* , matches the value stored in `$_SESSION`. If they differ, as in the case of the IDS attack, Drupal starts again a discovery on $URL.ID$ contained in t^* . The discovery returns the corresponding $URL.IdP$ and if these values do not match the $URL.IdP$ parameter stored in `$_SESSION`, t^* is not accepted.

To finally prevent the second discovery and to bypass the verification logic, we had to overwrite the `$_SESSION` variable. The attack is shown in Figure 7 and works as follows:

- (1.)-(3.) A login request with the attacker's account $URL.ID_A$ is started. Drupal discovers it and stores $URL.ID_A$ and $URL.IdP_A$ in `$_SESSION`.
- (4.) Drupal starts an association with IdP_A , which returns β (using KC strategy 2).

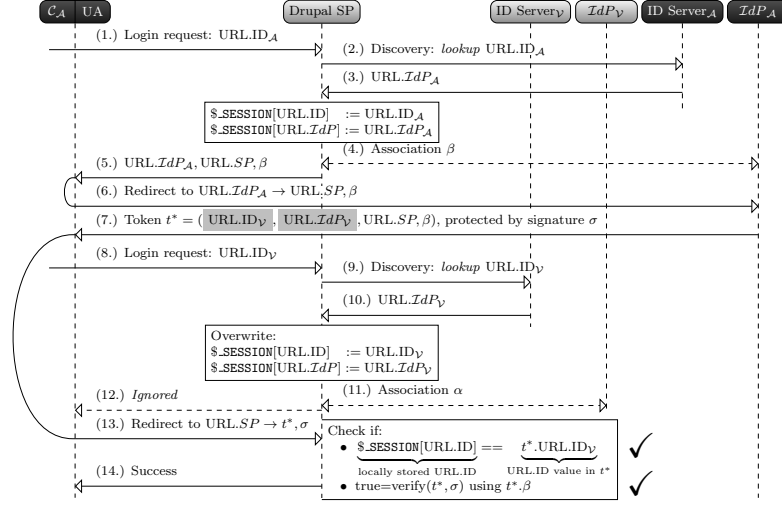


Fig. 7: Key Confusion attack on Drupal: Before the token t^* in Step (7.) is forwarded to Drupal in Step (13.), the attacker C_A starts a second login request in Step (8.) using the victim's identity $URL.ID_V$. This overwrites the $URL.ID$ and $URL.IdP$ data stored in $\$SESSION$ and prevents the second discovery.

- (5.)-(7.) Drupal redirects the attacker to $URL.IdP_A$. The OpenID Attacker IdP creates a token $t^* = (URL.ID_V, URL.IdP_V, URL.SP, \beta)$. Then, the attacker delays the sending of the token to Drupal.
- (8.)-(10.) The attacker submits a further login request to Drupal, but this time with the victim's identity $URL.ID_V$. Drupal starts a new discovery on it and receives $URL.IdP_V$. Both values, $URL.ID_V$ and $URL.IdP_V$, are then stored in $\$SESSION$, overwriting $URL.ID_A$ and $URL.IdP_A$.
- (11.) Drupal starts another association with IDP_V , which returns α .
- (12.) Drupal redirects the attacker to $URL.IdP_V$, but this redirect is not relevant for the attack.
- (13.)-(14.) The halted token t in (6.) is now sent to Drupal. Drupal verifies the signature. The interesting point at this step is that Drupal loaded the key from the database by only using β contained in t^* . It does not verify whether the association β was really established with $URL.IdP_V$. Thus, the signature is valid. Then, Drupal compares the values of $URL.ID_V$ and $URL.IdP_V$ contained in the token with the ones stored in $\$SESSION$. Because of being equal, there is no second discovery and we are logged in with the victim's identity.

We reported the issue to the Drupal security team and suggested to fix it by fetching the key via $(URL.IdP, \alpha/\beta)$ instead of using α/β only. They accepted

the idea and implemented it in their new release Drupal 8 as well as in Drupal 7 and Drupal 6 [10]. For a better understanding, we added a video as a demonstration of this attack that shows the usage of OpenID Attacker [34].

7.3 ID Spoofing

Six of the tested targets were vulnerable to IDS. Those targets did not check if the identity contained in the token was issued by the correct IdP.

Sourceforge.

Initially, we started a black-box testing and detected that the applied OpenID authentication is vulnerable against IDS. Figure 8 shows the log window of our developed OpenID Attacker tool which contains all exchanged OpenID parameters. Consequentially, we contacted the support team and described the issue. Later on, they answered us that vulnerability is fixed.

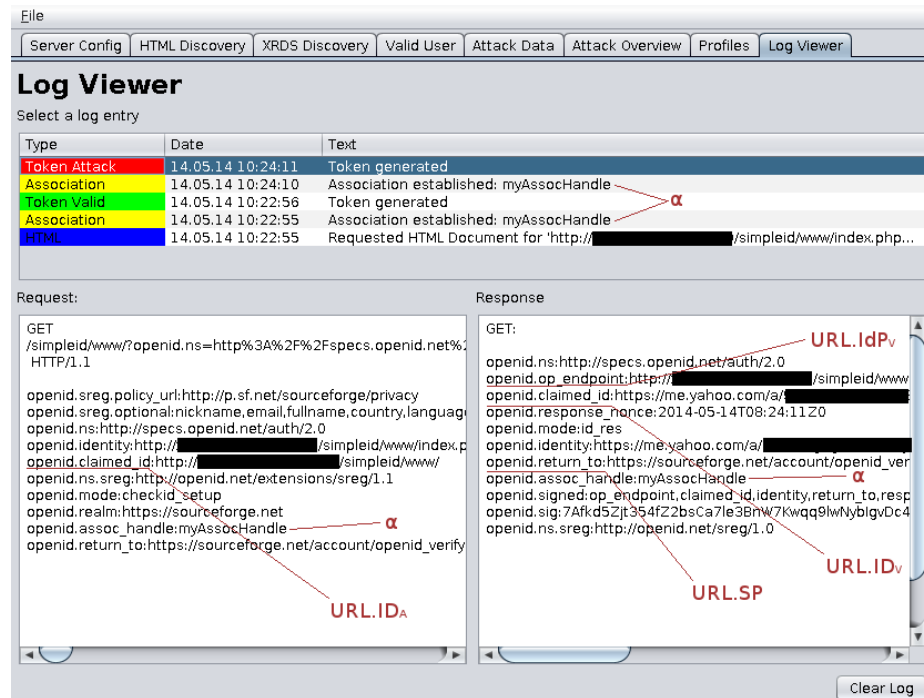


Fig. 8: IDS attack on Sourceforge. The OpenID Attacker *log viewer* window lists all exchanged OpenID messages. The Screenshot shows that the SP requests a token for URL.ID_A, but the tools ignores the wish and responds with a token for URL.ID_V.

We analyzed the implementation again. Using OpenID Attacker, we found out that the IDS attack was no longer working. Unfortunately, Sourceforge noticed that the identity contained in the OpenID token is different to the one requested during the login request. As a result, Sourceforge started to rediscover the submitted identity and the attack failed. Based on this information, we mounted the same attack technique as on Drupal: we confused Sourceforge with a second login request on URL.ID_V right after we submitted the login request for URL.ID_A . As expected, KC was applicable. Consequentially, we contacted the Sourceforge support team and described our finding.

Using only black-box testing we were able to determine that the implementation uses a session variable to connect the initial login request with the token response. In collaboration with the support team, we fixed the vulnerability. We suggested to fetch the key from the database not only by using α , but rather by a combination of $(\text{URL.ID}_P, \alpha)$. In this manner, KC can be prevented. The Sourceforge support team pointed out that the OpenID specification [23, Section 11.2] addresses this problem, but it only describes that a rediscovery is necessary in the given case. It neither addresses how to find out that the identity of the login request is not the same as in the token, nor mentions that this fact could be abused by attackers.

7.4 Discovery Spoofing

OwnCloud is up to now the only framework that is vulnerable to DS attacks. We nevertheless describe this attack because it allows us to utilize the discovery phase for the injection of identities, which are not controlled by our IdP, but used for the login.

ownCloud. OwnCloud [35] is a PHP-based, open source cloud framework. It provides universal access to files as a *self*-controlled alternative to Dropbox or Google Drive and additionally, ownCloud users' can sync private data such as contacts and calendar information. ownCloud allows SSO by simply activating the OpenID plugin, which is distributed by default with ownCloud 5.

There are two interesting parts in ownCloud's OpenID implementation: (1.) in comparison to other implementations, ownCloud always starts a rediscovery so that the KC attack is not applicable. (2.) ownCloud does not verify the token's signature itself. Instead, it uses the *check authentication* mechanism (see steps (12.) and (13.) in Figure 4) and sends the token to the IdP. This means that using OpenID Attacker to send, for example, a token for a Google account would lead ownCloud to send the token directly to a Google server for verification, which will not accept it. Thus, for attacking ownCloud we could not send a token containing URL.ID_V – the IDS and KC attacks are not possible.

By examining the OpenID's discovery phase, we found out that the OpenID specification allows the usage of an URL.ID value in the HTML/XRDS files. This feature can be used to trick ownCloud as shown in Figure 9.

When ownCloud receives the OpenID token in Step (5.), it performs a rediscovery on the contained identity. We configured the OpenID Attacker IdP to

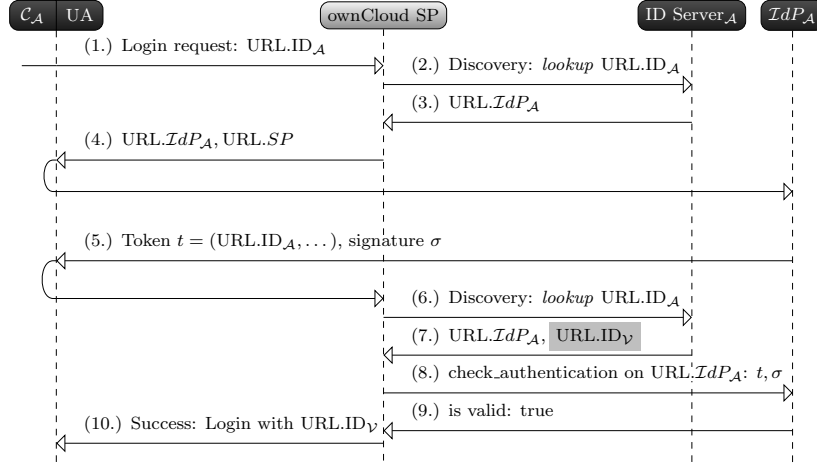


Fig. 9: The Discovery Spoofing attack on ownCloud: The attacker’s ID server returns URL.ID_V on the second discovery. ownCloud uses this identity value for the login instead of the identity provided within the token.

include the victim’s identity URL.ID_V in the discovered document of Step (7.) as shown in Listing 1.2 additionally to URL.IdP_A . Afterwards, ownCloud sends the token to the attacker’s IdP_A in Step (8.) by using the discovered URL.IdP_A and it returns that the token is valid in Step (9.). Surprisingly, instead of using the URL.ID_A contained in t to log in the user, ownCloud uses URL.ID_V returned in Step (7.). We were logged in with the victim’s identity.

We contacted the ownCloud security team and reported the issue. The ownCloud team acknowledged our work in [13].

7.5 Additional Findings

The findings described here did not result in a valid attack according to our model, but are worth reporting.

Unsigned OpenID Parameters. The OpenID specification [23, Section 10.1] requires the following parameters to be signed: `op_endpoint`, `return_to`, `response_nonce`, `assoc_handle`, `claimed_id` and `identity`. 4 of 16 targets (CFOpenID, OpenID CFC, OpenID 4 Node.js, Zend Framework) accept tokens in which some of these parameters were not signed, and could thus be forged by an attacker.

XML External Entity. We determined that 2 of 16 analyzed targets (OpenID CFC, Net::OpenID::Consumer) are susceptible to XXE attacks [36,37]. Additionally, we found out that Slashdot [38] (Alexa rank 1626) was vulnerable to XXE because of using the Net::OpenID::Consumer library. Slashdot acknowledged our findings in [14]

Replay Attack. OpenID has only one parameter containing a timestamp (`openid.response_nonce`). It contains the creation time of the token concatenated with a random string, but does not include an expiration time. Thus, the SP can decide on its own how long it accepts such a token.

The lifetime of a token is additionally limited by the lifetime of the association and the corresponding key. We found that this lifetime varies heavily: associations with Yahoo have a lifetime of 4 hours, with Google 13 hours, and with MyOpenID 14 days.

8 OpenID Attacker Implementing a malicious IdP

We developed *OpenID Attacker* as a part of our research and as a result of our token verification model for SPs. OpenID Attacker is an open source penetration test tool that mainly acts as an OpenID IdP and offers a Graphical User Interface (GUI) for easy configuration, see Figures 8 and 11. As such, it is able to operate during all three phases of the OpenID SSO protocol. OpenID Attacker is free, open source and can be downloaded here [22].

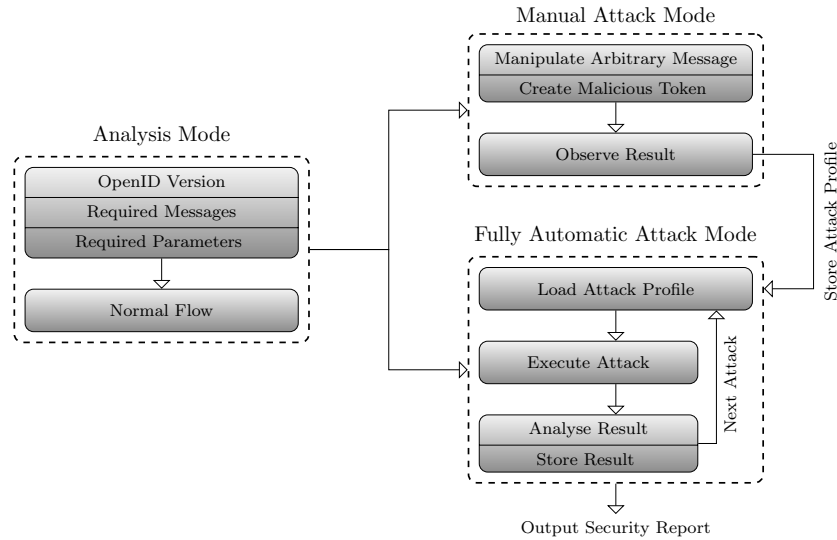


Fig. 10: The three modes of OpenID Attacker.

The main advantage of OpenID Attacker is its flexibility – the attacks can be provided manually or full automatically. As shown in Figure 10, OpenID Attacker works in three modes: (1.) Analysis, (2.) Manual Attack, (3.) Fully Automatic Attack.

Analysis Mode. In this mode OpenID Attacker is used to analyze the normal behavior of the target SP. For this purpose, OpenID Attacker acts as benign IdP and creates valid tokens. Additionally, it gets and stores information about the supported OpenID version on the SP, the exact message flow, for instance, which optional messages are used, the schema of the messages and the required parameters. Once calibrated, OpenID Attacker stores the collected informations in a data structure, called *Normal Flow*, used by the other modes.

In this mode OpenID Attacker works automatically and does not require any interaction or configuration.

Manual Attack Mode. In this mode, OpenID Attacker acts as a malicious IdP hand-operated by the attacker. The attacker starts the security analysis on basis of the informations stored in *Normal Flow*. He manipulates parameters in the messages and creates malicious tokens. He then observes the results of the attacks. In this mode, the attacks and the evaluation of the attacks are carried out manually.

The idea behind the *Manual Mode* is the fact that new attack vectors can be inspected. This is an important fact, because the *Manual Mode* allows to investigate the OpenID protocol very deeply and fine granular as every single aspect of the protocol can be manipulated. In combination with a running SP implementation in debugging mode, this mode helps to understand the source code of the SP to find implementation as well as protocol issues. We used this mode to discover the four novel OpenID attacks TRC, IDS, KC, DS during a white-box analysis. The configuration of the attack vectors can then be stored as an *Attack Profiles* (cf. Figure 11) and can later be loaded for black-box analysis. By using *Attack Profiles*, any of the stored attacks can be easily reproduced with only one click.

Full Automatic Attack Mode. In this mode OpenID Attacker acts as full automated malicious IdP penetration test tool. Initial, OpenID Attacker loads the stored *Attack Profiles* and the *Normal Flow*. Afterwards, it sequentially executes the attacks defined in the profiles. Then, OpenID Attacker analyzes the result of the attack and stores the information in the security report, see Figure 12. In conclusion, OpenID Attacker summarizes the results of all attacks contained in the *Attack Profiles* and creates a security report.

9 Related Work

Related work can be divided into three parts: research on analysis of SSO systems, specific investigations in the field of OpenID, and development of SSO testing tools. Please note that none of the previous papers considers malicious IdPs as part of the attacker, and none of the OpenID papers considered attacks on the association phase.

SSO Security. Various vulnerabilities have been found over the last two decades. In 2003 and 2006, Groß [5,6] analyzed the SAML Browser/Artifact profile and

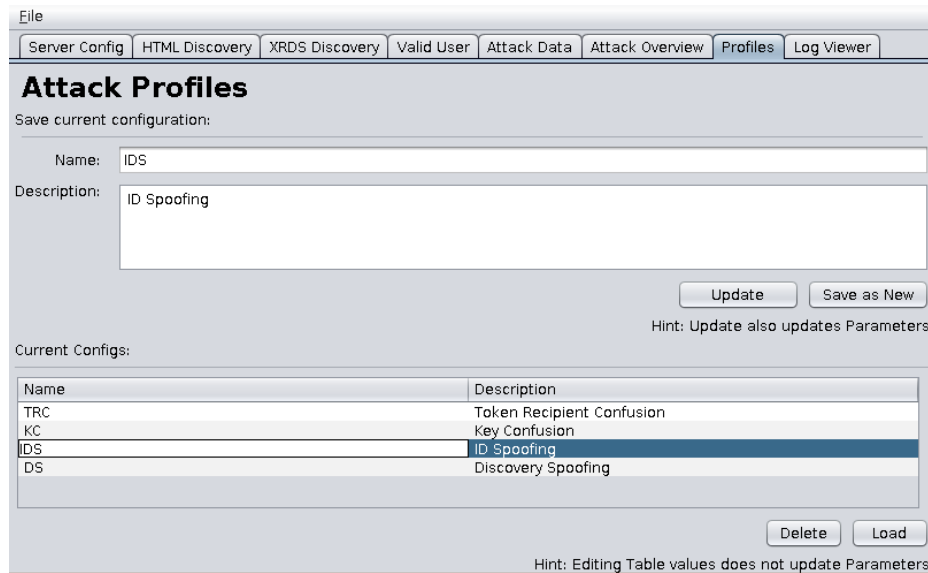


Fig. 11: The OpenID Attacker profile window allows to automatically chose an attack configuration for all four presented attacks. A video as a demonstration of the attack on Drupal showing the usage of OpenID Attacker can be found on [34].

Token Recipient Confusion			
#	Description	Log	Applicable
0	Modification of the openid.return_to value	Show Log	✗
ID Spoofing			
#	Description	Log	Applicable
0	claimed id is used	Show Log	✓
0	identity is used	Show Log	✓
0	ID Spoofing attack possible	Show Log	✗
Discovery Spoofing			
#	Description	Log	Applicable
0	XRDS Discovery Spoofing - OpenID 2.0	Show Log	✗
0	XRDS Discovery Spoofing - OpenID 1.0	Show Log	✗
0	HTML Discovery Spoofing - OpenID 2.0	Show Log	✗
0	HTML Discovery Spoofing - OpenID 1.0	Show Log	✗
Key Confusion			
#	Description	Log	Applicable
0	key confusion	Show Log	✓

Fig. 12: The *Fully Automatic Attack Mode* outputs a security report.

identified several flaws in the SAML specification that allow connection hijacking/replay attacks, as well as Man-in-the-Middle (MitM) attacks and HTTP

referrer attacks. We used these attacks as model for the TRC attack. In 2008 and 2011, Armando et al. [39,40] built a formal model of the SAML V2.0 Web Browser SSO protocol and analyzed it with the model checker SATMC. The authors found vulnerabilities in Google’s SAML interface. In 2012, Somorovsky et al. [24] investigated the XML Signature validation of several SAML frameworks. By using the XML Signature Wrapping (XSW) attack technique, they bypassed the authentication mechanism in 11 out of 14 SAML frameworks.

Sun et al. [41] analyzed the implementation of nearly 100 OAuth implementations, and found serious security flaws in many of them. Their research concentrated on classical web attacks like XSS, CSRF and TLS misconfigurations. Further security flaws in OAuth based applications were discovered by [42,43,44,45,46,47], whereby the authors concentrated on individual attacks. In 2013 Wang et al. introduced a systematic process for identifying critical assumptions in SDKs, which led to the identification of exploits in constructed apps resulting in changes in the OAuth 2.0 specification [48]. Chen et al. revealed in 2014 serious vulnerabilities in OAuth applications on mobile devices caused by the developer’s misinterpretation of the OAuth protocol [49].

In 2014 Fett et al. [50] built a formal model of the BrowserID protocol [51], which allows them to remodel known weaknesses and vulnerabilities in BrowserID.

OpenID Security. The analysis of the OpenID protocol started with version 1.0. Eugene Tsyurklevich and Vlad Tsyurklevich [52] presented several attacks on this OpenID version at Black Hat in 2007. They identified, for instance, a threat in the IdP endpoint URL (*URL.IdP*) published within the discovery phase. It can point to critical files on the local machine or can even be abused in order to start a Denial-of-Service (DoS) attack by enforcing the SP to download a large movie file. Comparable to [41], they also looked at replay and CSRF attacks. In 2008, Newman and Lingamneni [53] created a model checker for OpenID 2.0, but for simplicity, they removed the association phase out of their model. By using it, they could identify a session swapping vulnerability, which enforces the victim to log in into attacker’s account on an SP. In this manner, an attacker could eavesdrop the victim’s activities. In comparison to our work, the attacks presented in [53] do not result in unauthorized access. Interestingly, the authors of the paper modeled an IdP capable to make associations with legitimate SPs. However, they did not consider a dishonest IdP capable to start attacks like IDS and DS. Since KC is related to the association phase, the attack was not covered by the model checker. Later on, Sun et al. [54] provide a comprehensive formal analysis on OpenID and an empirical evaluation of 132 popular websites. The authors investigated CSRF, Man-in-the-middle attacks and the SSL support of OpenID implementations. In contrast to our work, they assumed that the SP and the IdP were trustworthy, so that they could not identify any of the attacks presented in this paper.

Finally, Wang et al. [7] concentrated on real-life SSO systems instead of a formal analysis. They have well demonstrated the problems related to token verification with different attacks. They developed a tool named BRM-Analyzer that handles the SP and IdP as black-boxes by analyzing only the traffic visible

within the browser. Their paper served as a model for our research. However, the BRM-Analyzer is rather passive (it analyzes the browser related messages), while OpenID Attacker acts as an IdP and as such, it can actively interfere with the OpenID workflow (e.g. create SSO tokens).

In 2014, Silva et al. [37] exploited an XML External Entity vulnerability in Facebook’s parsing mechanism of XRDS documents during the discovery phase. The same attack is supported by the OpenID Attacker and is part of our evaluation. Simultaneously to our research, in 2014 Wang et al. [55] reported serious flaws in OAuth and OpenID, which are related to TRC.

SSO Security Tools. In 2013, Bai et al. [56] have proposed AuthScan, a framework to extract the authentication protocol specifications automatically from implementations. They found security flaws in several SSO systems. The authors concentrated on MitM attacks, Replay attacks and Guessable tokens. More complex attacks, like IDS or KC, cannot be evaluated. In the same year, Wang et al. [57] developed a tool named *InteGuard* detecting the invariance in the communication between the client and SP to prevent logical flaws in the latter one. Another tool similar to *InteGuard* is *BLOCK* [58], which acts as a proxy and examines to the invariance of web related messages. Both tools should be able to detect Replay attacks and TRC. Since all HTTP messages between the adversary and the SP are valid and do not show abnormalities, neither *InteGuard* nor *BLOCK* is able to mitigate IDS, DS, KC and XML External Entity. Evans et al. [47] published on USENIX’14 a fully automated tool named *SSOScan* for analyzing the security of OAuth implementations and described five attacks, which can be automatically tested by the tool.

10 Lessons Learned

Trusted IdPs. When Microsoft introduced MS Passport, the first web SSO system, criticism concentrated on the closed nature of the system: only a single IdP at the domain `passport.com` was used. Thus subsequent approaches like MS Cardspace and SAML Web SSO allowed multiple IdPs, but still retained the idea that an IdP should only be run by trusted parties, and that a trust relationship between a SP and an IdP should be established manually. With OpenID, “openness” for the first time became more important than “trustworthiness”, and this resulted in new attack classes. The lesson learned is that the establishment of trust should not be fully automated, if this isn’t backed up by solid cryptography (like e.g. in PKI scenarios).

Identities are Important. Attacks similar to TRC have been described before in the literature. E.g. Armado et al. discovered a bug in the Google SSO implementation where the identity of the target SP was omitted from the SAML assertion. Thus an assertion issued for (low-security) service A (controlled by the attacker) could be used to log into (high-security) service B. Including identities in protocol messages, and checking these values, is good engineering practice, e.g. in TLS certificate verification. The lesson learned from the TRC attack is

that checking identity of the SP is always important and should be enforced in any application.

References to Cryptographic Keys. KC exploits weaknesses in the association between the identity of the IdP, the key handle and the key value used for the signature verification. In OpenID the only connection between the key and the corresponding IdP is the association handle α . Unfortunately, the value of α can be freely chosen by *any* IdP. In case of OpenID, if the loading of the key occurs only on basis of α and without verifying the corresponding IdP, KC is applicable. Lessons learned: The identification of the correct cryptographic keys should be unambiguous. If keys are related to the identity of a communicating party, then this identity should be part of the key identifier. E.g., keys should be stored indexed by a pair (IdP_{ID}, α) .

Multiple Equivalent Parameters. If two or more different parameters are used for the same purpose, then it is difficult to formally specify how to react if these two parameters have different semantics. This fact was exploited in the Discovery Spoofing attack, which is only possible if two different strings are used as identifiers for the same entity. Similar problems have been reported in multi-layer messaging: E.g. in SOAPAction Spoofing, the SOAP action can be specified in the HTTP and in the SOAP Header. By specifying two different values, inconsistent behaviour from the SOAP receiver can be triggered.

Complex Information Flow Specification. In many cases, developers of OpenID frameworks deviated from the specification, which resulted in a different, vulnerable message flow. It seems that the OpenID specification is not clear enough to unambiguously implement the desired message flow. It is an interesting open question how to formally specify the desired flow, such that computer-aided enforcement of this flow, or computer-aided checking of this flow, becomes possible.

11 Future Work

We showed that SSO protocols and implementations are a high-value attack target. Although there is a lot of research in the area of SSO [41,24,47] and OpenID [7,54,59], the number of vulnerabilities found is surprisingly high.

We believe that the concept of a malicious IdP is a threat to all open SSO protocols, thus future work includes applying the methodology developed in this paper to different protocols like OAuth, SAML and OpenID Connect.

We will make the source code of OpenID Attacker public, encouraging researchers and penetration tester to use this tool to further improve security in SSO systems, and to adapt it to other protocols.

12 Acknowledgments

The authors would like to thank Juraj Somorovsky for fruitful discussions and the motivation to go on further and deep on this topic. We additionally want

to thank Christian Kossmann for the extension of OpenID Attacker to support fully automatic OpenID attacks.

References

1. D. Silver, S. Jana, E. Chen, C. Jackson, and D. Boneh, "Password managers: Attacks and defenses," in *Proceedings of the 23rd Usenix Security Symposium*, 2014.
2. Z. Li, W. He, D. Akhawe, and D. Song, "The emperor's new password manager: Security analysis of web-based password managers," in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014.
3. Janrain. (2013) 2013 consumer research: The value of social login. Janrain. [Online]. Available: <http://janrain.com/resources/industry-research/2013-consumer-research-value-of-social-login/>
4. BuiltWith, "Openid usage statistics," 2014. [Online]. Available: <http://trends.builtwith.com/docinfo/OpenID>
5. T. Groß, "Security analysis of the saml single sign-on browser/artifact profile," in *Computer Security Applications Conference, 2003. Proceedings. 19th Annual. IEEE*, 2003, pp. 298–307.
6. T. Groß and B. Pfitzmann, "SAML artifact information flow revisited," Research Report RZ 3643 (99653), IBM Research, 2006, <http://www.zurich.ibm.com/security/publications/2006.html>.
7. R. Wang, S. Chen, and X. Wang, "Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, ser. SP '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 365–379. [Online]. Available: <http://dx.doi.org/10.1109/SP.2012.30>
8. A. Barth, C. Jackson, and J. C. Mitchell, "Securing frame communication in browsers," in *In Proceedings of the 17th USENIX Security Symposium*, 2008.
9. OpenID, "Openid libraries," 2014. [Online]. Available: <http://wiki.openid.net/w/page/12995176/Libraries>
10. V. M. Christian Mainka, "CVE-2014-1475," <http://www.cvedetails.com>, 2014. [Online]. Available: <http://www.cvedetails.com>
11. —, "CVE-2014-2048," 2014. [Online]. Available: <http://www.cvedetails.com>
12. —, "Fixing id spoofing and recipient confusion in joid," 2014. [Online]. Available: <https://code.google.com/p/joid/source/detail?r=220>
13. —, "Insecure openid implementation (oc-sa-2014-002)," 2014. [Online]. Available: <http://owncloud.org/security/advisory/?id=oC-SA-2014-002>
14. —, "Slashdot acknowledgement," 2014. [Online]. Available: <http://beta.slashdot.org/journal/1083427>
15. —, "CVE-2014-8249," 2014. [Online]. Available: <http://www.cvedetails.com>
16. —, "CVE-2014-8250," 2014. [Online]. Available: <http://www.cvedetails.com>
17. —, "CVE-2014-8251," 2014. [Online]. Available: <http://www.cvedetails.com>
18. —, "CVE-2014-8252," 2014. [Online]. Available: <http://www.cvedetails.com>
19. —, "CVE-2014-8253," 2014. [Online]. Available: <http://www.cvedetails.com>
20. —, "CVE-2014-8254," 2014. [Online]. Available: <http://www.cvedetails.com>
21. —, "CVE-2014-8265," 2014. [Online]. Available: <http://www.cvedetails.com>
22. —, "Openid attacker, source code and executable, will be available for the public on the day of acceptance," 2014. [Online]. Available: <https://www.dropbox.com/s/z67fa3qcte6jdga/OpenID-Attacker.zip>

23. specs@openid.net, “OpenID Authentication 2.0 – Final,” Dec. 2007. [Online]. Available: https://openid.net/specs/openid-authentication-2_0.html
24. J. Somorovsky, A. Mayer, J. Schwenk, M. Kampmann, and M. Jensen, “On breaking saml: Be whoever you want to be,” in *Proceedings of the 21st USENIX conference on Security symposium, Security*, vol. 12, 2012, pp. 21–21.
25. S. Cantor et al., “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0,” <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>, Mar. 2005.
26. C. Mainka, V. Mladenov, F. Feldmann, J. Krautwald, and J. Schwenk, “Your software at my service: Security analysis of saas single sign-on solutions in the cloud,” in *Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security*, ser. CCSW ’14. New York, NY, USA: ACM, 2014, pp. 93–104. [Online]. Available: <http://doi.acm.org/10.1145/2664168.2664172>
27. D. Hardt, “The OAuth 2.0 Authorization Framework,” RFC 6749 (Proposed Standard), Internet Engineering Task Force, Oct. 2012. [Online]. Available: <http://www.ietf.org/rfc/rfc6749.txt>
28. S. Cantor et al., “Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0,” Mar. 2005. [Online]. Available: <http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf>
29. Dice Holdings, Inc., “SourceForge,” 2014. [Online]. Available: <https://sourceforge.net/>
30. Amazon.com Inc., “Alexa Analytics for any Website,” 2014, [online] <http://www.alexa.com/>. [Online]. Available: <http://www.alexa.com/>
31. B. Ferg and G. Krall, “JOID,” 2014, [online] <https://code.google.com/p/joid/>. [Online]. Available: <https://code.google.com/p/joid/>
32. Drupal Team and D. Buytaert, “Drupal Open Source CMS,” 2014. [Online]. Available: <https://drupal.org/>
33. W3Techs – World Wide Web Technology Surveys, “Usage of content management systems for websites,” 2014, accessed: 05.11.2014. [Online]. Available: http://w3techs.com/technologies/overview/content_management/all/
34. V. M. Christian Mainka, “ScreenCast: Attacking drupal 7 with key confusion,” 2014, [online] https://www.dropbox.com/s/5np7hpujyx4fd/Attacking_Drupal7.mpg [MPEG2, 2:09min, 54mb]. [Online]. Available: <https://www.dropbox.com/s/z67fa3qcte6jdga/OpenID-Attacker.zip>
35. ownCloud Inc., “ownCloud,” 2014. [Online]. Available: <http://owncloud.org/>
36. G. Steuck, “XXE (Xml eXternal Entity) Attack,” OWASP, October 2002. [Online]. Available: <http://www.securiteam.com/securitynews/6D0100A5PU.html>
37. R. Silva. (2014, 01) XXE in OpenID: one bug to rule them all, or how I found a Remote Code Execution flaw affecting Facebook’s servers. http://www.ubercomp.com/posts/2014-01-16_facebook_remote_code_execution.
38. Slashdot, “SlashDot.org,” 2014. [Online]. Available: <http://slashdot.org/>
39. A. Armando, R. Carbone, L. Compagna, J. Cuéllar, and M. L. Tobarra, “Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps,” in *Proceedings of the 6th ACM Workshop on Formal Methods in Security Engineering, FMSE 2008*, V. Shmatikov, Ed. Alexandria and VA and USA: ACM, 2008, pp. 1–10.
40. A. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino, and A. Sorniotti, “From Multiple Credentials to Browser-Based Single Sign-On: Are We More Secure?” in *SEC*, ser. IFIP Advances in Information and Communication Technology, J. Camenisch, S. Fischer-Hübner, Y. Murayama, A. Portmann, and C. Rieder, Eds., vol. 354. Springer, 2011, pp. 68–79.

41. S.-T. Sun and K. Beznosov, "The devil is in the (implementation) details: an empirical analysis of oauth sso systems," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 378–390.
42. Egor Homakov. (2014, February) How I hacked Github again.
43. —. (2013, February) How we hacked Facebook with OAuth2 and Chrome bugs. [Online]. Available: <http://homakov.blogspot.ca/2013/02/hacking-facebook-with-oauth2-and-chrome.html>
44. —. (2013, March) OAuth1, OAuth2, OAuth...?
45. Nir Goldshlager. (2013, February) How I Hacked Facebook OAuth To Get Full Permission On Any Facebook Account (Without App "Allow" Interaction). [Online]. Available: <http://www.nirgoldshlager.com/2013/02/how-i-hacked-facebook-oauth-to-get-full.html>
46. —. (2013, March) How I Hacked Any Facebook Account...Again! [Online]. Available: <http://www.nirgoldshlager.com/2013/03/how-i-hacked-any-facebook-accountagain.html>
47. D. E. Yuchen Zhou, "Automated testing of web applications for single sign-on vulnerabilities," in *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, Aug. 2014. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/zhou>
48. R. Wang, Y. Zhou, S. Chen, S. Qadeer, D. Evans, and Y. Gurevich, "Explicating sdks: Uncovering assumptions underlying secure authentication and authorization," in *Proceedings of the 22Nd USENIX Conference on Security*, ser. SEC'13. Berkeley, CA, USA: USENIX Association, 2013, pp. 399–414. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2534766.2534801>
49. E. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague, "OAuth demystied for mobile application developers," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. ACM – Association for Computing Machinery, November 2014. [Online]. Available: <http://research.microsoft.com/apps/pubs/default.aspx?id=231728>
50. D. Fett, R. Küsters, and G. Schmitz, "Paper: An Expressive Model for the Web Infrastructure: Definition and Application to the BrowserID SSO System," in *35th IEEE Symposium on Security and Privacy (S&P 2014)*. IEEE Computer Society, 2014.
51. M. Corporation, "Browserid specification," https://openid.net/specs/openid-authentication-2_0.html, <http://www.mozilla.org>, Tech. Rep., 2011. [Online]. Available: <https://github.com/mozilla/id-specs/blob/prod/browserid/index.md>
52. E. Tsyklevich and V. Tsyklevich, "Single sign-on for the internet: A security story," July and August 2007. [Online]. Available: <https://www.blackhat.com/presentations/bh-usa-07/Tsyklevich/Whitepaper/bh-usa-07-tsyklevich-WP.pdf>
53. B. Newman and S. Lingamneni, "Cs259 final project: Openid (session swapping attack)," 2008. [Online]. Available: <http://www.stanford.edu/class/cs259/projects/cs259-final-newmanb-slingamn/report.pdf>
54. S.-T. Sun, K. Hawkey, and K. Beznosov, "Systematically breaking and fixing openid security: Formal analysis, semi-automated empirical evaluation, and practical countermeasures." *Computers & Security*, vol. 31, no. 4, pp. 465–483, 2012. [Online]. Available: <http://dblp.uni-trier.de/db/journals/compsec/compsec31.html#SunHB12>
55. W. Jing. (2014, 2 May) Serious security flaw in oauth, openid discovered. <http://www.cnet.com/news/serious-security-flaw-in-oauth-and-openid-discovered/>. Ph.D. student at the Nanyang Technological University in

- Singapore. [Online]. Available: <http://www.cnet.com/news/serious-security-flaw-in-oauth-and-openid-discovered/>
56. G. Bai, J. Lei, G. Meng, S. S. Venkatraman, P. Saxena, J. Sun, Y. Liu, and J. S. Dong, "Authscan: Automatic extraction of web authentication protocols from implementations," *NDSS, February*, 2013.
 57. L. Xing, Y. Chen, X. Wang, and S. Chen, "Integuard: Toward automatic protection of third-party web service integrations," in *Proceedings of 20th Annual Network & Distributed System Security Symposium*, 2013.
 58. X. Li and Y. Xue, "Block: A black-box approach for detection of state violation attacks towards web applications," in *Proceedings of the 27th Annual Computer Security Applications Conference*, ser. ACSAC '11. New York, NY, USA: ACM, 2011, pp. 247–256. [Online]. Available: <http://doi.acm.org/10.1145/2076732.2076767>
 59. P. Sovis, F. Kohlar, and J. Schwenk, "Security analysis of openid." in *Sicherheit*, ser. LNI, F. C. Freiling, Ed., vol. 170. GI, 2010, pp. 329–340. [Online]. Available: <http://dblp.uni-trier.de/db/conf/sicherheit/sicherheit2010.html#SovisKS10>

Service Provider	Program- ming Language	TRC	KC	IDS	DS	Summary: Unauthor- ized Access
CF OpenID	ColdFusion		-		-	
DotNet OpenAuth	.NET	-	-	-	-	-
Drupal 6 / Drupal 7	PHP	-		-	-	
dyuproject	Java		-		-	
janrain	PHP, Python, Ruby	-	-	-	-	-
JOID	Java		-		-	
JOOpenID	Java	-	-		-	
libopkele (Apache mod_auth_openid)	C++	-	-	-	-	-
LightOpenID	PHP	-	-	-	-	-
Net::OpenID::Consumer	Perl		-	-	-	
OpenID 4 Java (WSO2)	Java	-	-	-	-	-
OpenID CFC	ColdFusion	-	-		-	
OpenID for Node.js (everyauth, Passport)	JavaScript/NodeJS		-	-	-	
Simple OpenID PHP Class (ownCloud 5)	PHP		-	-		
Sourceforge	n.a.	-			-	
Zend Framework OpenID Component	PHP	-		-	-	
Total		6	3	6	1	11/ 16

One account on the target is compromised.

All accounts on the target are compromised.

Table 1: Results of our practical evaluation. For eleven out of 16 targets, we could get *unauthorized access*. Three targets were compromised using the web attacker model (). The other eight targets make use of a weaker variant (), *without any user interaction*.

Notation	Explanation
URL.ID	A URL representing a user's <i>login name</i>
URL.ID _C	A URL representing C's <i>login name</i> at URL.IdP _C
URL.ID _A	A URL representing A's <i>login name</i> at URL.IdP _A
URL.SP	The URL of the SP, e.g. http://mysp.com
URL.SP _A	The URL of the attacker A controlled SP, e.g. http://sp.attacker.com
URL.IdP	The URL of the user's IdP, e.g. https://www.google.com/accounts/o8/ud
URL.IdP _C	The URL of C's IdP, e.g. https://www.google.com/accounts/o8/ud .
URL.IdP _A	The URL of the attacker A controlled IdP, e.g. http://idp.attack.com .
t	The OpenID token, containing at least URL.ID, URL.SP and URL.IdP.
σ	The signature value for token t .
α	The value α is used to identify the key to verify (t, σ) . Note that α is just a reference value to the key and does not contain any key material. For the attack on Drupal, we also used β , because there are two different associations.

Table 2: List of notations used in this paper.